NorthTec
TAI TOKERAU WĀNANGA

# *POLICY*
# ICT RESOURCE SECURITY MANAGEMENT
# (03.008)

**POLICY**
Northland Polytechnic shall protect ICT resources from all threats, whether deliberate or accidental.

**PURPOSE**
To ensure business continuity and minimise the impact of security breaches.

**APPLICATION AND SCOPE**

This policy applies to all Northland Polytechnic ICT resources, staff, students and visitors.

**DEFINITIONS**

- *Availability*
  Ensure that authorised users have access to information when required
- *Confidentiality*
  Ensure that information is accessible only to those authorised to have access
- *ICT Resources*
- Hardware and software including, but not limited to:
  - Data and communication network (LAN, WAN, Internet, and Wireless).
  - Computer and equipment (i.e. servers, computers, printers, multi-function devices, telephones, mobile devices)
  - Data storage media (i.e. backup tape, flash memory, removable hard disk) and data files.
  - Business applications and software licences.
- *Information security*
  Protect information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction
- *Information security management*
  Describe controls that an organisation needs to implement to ensure that it is appropriate to manage risks
- *Integrity*
  Safeguard the accuracy and completeness of information and processing methods
- *Security incident*
  An event (e.g. unauthorised access, theft, computer virus, illegal use of software, user errors, software failure) causes or has potential to cause a breach of information security
- *Security threat*
  A potential event may result in harm to a system or the Polytechnic. Threats may be deliberate (e.g. theft, unauthorised use of storage media), accidental (e.g. user error, network component failure), or environmental (e.g. earthquake, lightning)

- *User*
  A user must be a current Northland Polytechnic staff member or a currently enrolled student. Other individuals may also become users (with guest accounts) for Northland Polytechnic business purposes; examples include someone providing service to Northland Polytechnic and official visitors

**COMPLIANCE OBLIGATIONS**

*Auditor General*
*Copyright (Infringing File Sharing) Amendment Act 2011*

| | |
|---|---|
| **Responsibility** | Executive manager with responsibility for ICT |
| **Approval dates** | August 2015 |
| **Next Review** | August 2021 |

**OTHER RELATED DOCUMENTS**

Policy: *Acceptable use of ICT Resources (03.006)*

**APPENDIX 1**

**PROCEDURES AND GUIDELINES**

**1.0 In compliance with this policy all computer users and departments shall ensure:**

- Appropriate protection over the Polytechnic's ICT resources;
- Information and information processing facilities are physically protected from security threats and environmental hazards;
- The safeguarding of information in networks and the protection of the supporting infrastructure and services;
- That access to information and business processes are controlled on the basis of the polytechnic security requirements;
- That users are made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and safe use of information resources;
- Information security is maintained when using alternative types of information technology and electronic devices (different from the Polytechnic's standard computing and network environment);
- That information security is maintained when mobile computing equipment (e.g. Smart cell phones, laptops) and remote access facilities are used;
- Incidents affecting security are reported through appropriate management channels as quickly as possible;
- That adequate user security awareness and training is provided;
- The use of information systems in compliance with legislative and contractual requirements.

**2.0 Library, Flexible Learning and ICT shall ensure:**

- That formal procedures are in place to control the allocation of access rights to information systems and services;
- Adequate access controls are in place to prevent unauthorised access to the network, computers, and information held in information systems;
- That monitor mechanism is in place to detect deviation from access control policy and record system access events to provide evidence in case of security incidents;
- That all installations, implementation and maintenance of new or updated software and hardware on main Polytechnic network are controlled and will result in continued system operations, including availability and integrity of information;
- That application and system evaluation, testing, and development are conducted in an isolated environment that is separated from main Polytechnic network;
- Procedures and controls are in place to protect the integrity of software and information (e.g. Prevent and detect malicious software, virus, worms, and Trojan horses);
- That business continuity processes are implemented and maintained to reduce the disruption caused by disasters and security failures;

- That backup and recovery procedures are appropriately implemented and critical backup media are kept in a secured place offsite;
- Disaster recovery plans are appropriately documented and recovery tests are conducted regularly;
- That appropriate management processes are in place to handle security violations;
- The security of information systems is regularly reviewed and audited against the appropriate polytechnic policies, best practices and standards.

**KEYWORDS**

| REVISION HISTORY | | | |
|---|---|---|---|
| Version | Description of Change | Author | Effective date |
| 1 | New – replaced T05/01 (*Information Security Management)* | QMS Team | January 2009 |
| 2 | Review – management structure changes | QMS Team | January 2010 |
| 3 | Re-approval | P Brimacombe | August 2015 |
| 4 | Triennial review – no changes | S Milner | August 2018 |